# Configurar a segurança RADIUS IPSec para WLCs e Microsoft Windows 2003 IAS Server

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Configuração de IPSec RADIUS Configurar o WLC Configurar o IAS Configurações de segurança de domínio do Microsoft Windows 2003 Eventos de Log do Sistema do Windows 2003 Exemplo de depuração bem-sucedida de IPSec RADIUS do controlador de LAN sem fio Captura ética Informações Relacionadas

## **Introduction**

Este guia documenta como configurar o recurso RADIUS IPSec suportado pelo WCS e estas controladoras WLAN:

- 4400 Series
- WiSM
- 3750 G

O recurso IPSec RADIUS da controladora está localizado na GUI da controladora na seção Security > AAA > RADIUS Authentication Servers. O recurso fornece um método para criptografar todas as comunicações RADIUS entre controladores e servidores RADIUS (IAS) com IPSec.

# **Prerequisites**

### **Requirements**

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento sobre o LWAPP
- Conhecimento sobre autenticação RADIUS e IPSec
- Conhecimento sobre como configurar serviços no sistema operacional Windows 2003 Server

#### **Componentes Utilizados**

Esses componentes de rede e software devem ser instalados e configurados para implantar o recurso IPSec RADIUS do controlador:

- Controladores WLC 4400, WiSM ou 3750G. Este exemplo usa a WLC 4400 que executa a versão de software 5.2.178.0
- Pontos de Acesso Lightweight (LAPs). Este exemplo usa o LAP da série 1231.
- Switch com DHCP
- Servidor Microsoft 2003 configurado como um Controlador de Domínio instalado com a Autoridade de Certificação da Microsoft e com o IAS (Serviço de Autenticação da Internet) da Microsoft.
- Segurança de Domínio da Microsoft
- Adaptador cliente sem fio Cisco 802.11 a/b/g com ADU versão 3.6 configurado com WPA2/PEAP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### **Conventions**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

# Configuração de IPSec RADIUS

Este guia de configuração não aborda a instalação ou a configuração do Microsoft WinServer, da Autoridade de Certificação, do Ative Diretory ou do cliente WLAN 802.1x. Esses componentes devem ser instalados e configurados antes da implantação do recurso RADIUS IPSec do controlador. O restante deste guia documenta como configurar o IPSec RADIUS nestes componentes:

- 1. Controladores Cisco WLAN
- 2. IAS do Windows 2003
- 3. Configurações de Segurança de Domínio do Microsoft Windows

#### **Configurar o WLC**

Esta seção explica como configurar o IPSec no WLC através da GUI.

Na GUI do controlador, conclua estas etapas.

 Navegue até a guia Security > AAA > RADIUS Authentication na GUI da controladora e adicione um novo servidor RADIUS.

Cisco Systems	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C (
Security	RADIUS	Authenticatio	n Servers				
AAA General	Call Stat	ion ID Type	IP Address	~			
RADIUS Authentication RADIUS Accounting Local Net Users	Credenti	als Caching					
MAC Filtering Disabled Clients User Login Policies	Use AES	Key Wrap					
AP Policies	Network User	Management	Server Index	Server Address	Port	IPSec	
IDSec Certificates			1	192.168.30.10	1812	Disabled	
CA Certificate			3	192.168.30.105	1812	Enabled	

 Configure o endereço IP, a porta 1812 e um segredo compartilhado do novo servidor RADIUS. Marque a caixa de seleção IPSec Enable-, configure esses parâmetros de IPSec e clique em Apply.Observação: o segredo compartilhado é usado para autenticar o servidor RADIUS e como a chave pré-compartilhada (PSK) para autenticação IPSec.

Cisco Systems within withs	MONITOR WLANS CONTR	ROLLER WIRELESS SECURITY	MANAGEMEN
Security	Shared Secret		]
AAA General RADIUS Authentication	Confirm Shared Secret	•••	
RADIUS Accounting Local Net Users MAC Filtering	Key Wrap		
Disabled Clients User Login Policies	Port Number	1812	
AP Policies Access Control Lists	Server Status	Enabled 💙	
IPSec Certificates CA Certificate	Support for RFC 3576	Disabled 💙	
ID Certificate	Retransmit Timeout	2 seconds	
Web Auth Certificate			
Wireless Protection Policies	Network User	🗹 Enable	
Trusted AP Policies Rogue Policies Standard Signatures	Management	🗹 Enable	
Custom Signatures Client Exclusion Policies	IPSec	Enable	
AP Authentication	IPsec Parameters		
	IPSec	HMAC SHA1 💟	
	IPSEC Encryption	3DES 💙	
	(Shared Seceret will be used	as the Preshared Key)	
	IKE Phase 1	Main 🛩	
	Lifetime (seconds)	28800	
	IKE Diffie Hellman Group	Group 2 (1024 bits) 🔽	

## **Configurar o IAS**

Conclua estes passos no IAS:

1. Navegue até o gerenciador IAS no Win2003 e adicione um novo Cliente RADIUS.

Elle Action View Help				
⇔ → 🗈 🖬 🕷 🚱 🔮				
Internet Authentication Service (Local)	Friendly Name	Address	Protocol	Client-Vendor
Carl RADIUS Clients     Carl Remote Access Logging     Semote Access Policies	<u>]</u> 4404	192,168.30.2	RADIUS	RADIUS Standard
Connection Request Processing				

2. Configure as propriedades do cliente RADIUS com o endereço IP e o segredo compartilhado configurados no

	4404 Properties	? ×
	Settings	
	Eriendly name:	
	4404	
	Address (IP or DNS):	
	192.168.30.2	
	⊻erify	
	If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.	
	Client-Vendor: RADIUS Standard	
	Bequest must contain the Message Authenticator attribute	
	Shared secret:	
	Confirm shared secret:	
Controlador:	OK Cancel Ar	ylqc

3. Configure uma nova Política de Acesso Remoto para o Controlador:

bild for the second service for the service se			
Elle Action Yiew Help			
← → 💽 🖬 🕼 🖧 😫			
Internet Authentication Service (Local)	Name	Order	
RADIUS Clients	\$\$ 4404	1	
Remote Access Policies     Connection Request Processing			

4. Edite as propriedades da Política de Acesso Remoto do Controlador. Certifique-se de adicionar o NAS-Port Type - Wireless - IEEE

04 Properties	NAS-Port-Type		?
Settings	A <u>v</u> ailable types:		Selected types:
Specify the conditions that connection requests must match. Policy gonditions:          NAS-Port-Type matches "Ethernet OR Wireless - IEEE 802.11 DR Wireless         Add         Edt         Bemove         If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.	ADSL-CAP - Asymmetri ADSL-DMT - Asymmetri Async (Modem) Cable FDDI G.3 Fax HDLC Clear Channel IDSL - ISDN Digital Su ISDN Async V.110 ISDN Async V.120 ISDN Sync	<u>A</u> dd >> << <u>B</u> emove	Ethernet Wireless - IEEE 802.11 Wireless - Other
Edit Profile Unless individual access permissions are specified in the user profile, this policy controls access to the network.			
If a connection request matches the specified conditions: C Degy remote access permission G Grant remote access permission	Recycle Bn		
OK Cancel Apply			

5. Clique em **Edit Profile**, clique na guia **Authentication** e marque MS-CHAP v2 para Authentication:

Specifu the condit	it Dial-in Profile		1
Policy <u>c</u> onditions: NAS-Port-Type n	Dial-in Constraints Authentication	IP Encryption whods you want to allo	Multilink Advanced
▲	EAP Methods		2010 01145 - 21
<u>Add</u>	Microsoft Encrypted A	uthentication version 3	2 (MS-CHAP V2)
t connection requ associated profile	Microsoft Encrypted A	je password arter it na uthentication (MS-CH/	s expirea AP)
Edit <u>P</u> rofile	🗖 Uger can chang	re password after it ha	s expired
Jnless individual	Encrypted authenticat	ion (CHAP)	
controls ac	Unencrypted authention	cation (PAP, SPAP)	
f a connection re	Unauthenticated access-		
Grant remote .	Allo <u>w</u> clients to connect method.	ct without negotiating	an authentication

6. Clique em **Métodos EAP**, selecione Provedores EAP e adicione o PEAP como um tipo EAP:

dit Dial-in Profile		?	×	
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced		
Select the authentication	methods you want to allo	ow for this connection.		
EAP Methods				
Microsoft Encrypt	elect EAP Providers			? ×
🗖 User can <u>c</u>	EAP types are negotiate	ed in the order in which the	y are listed.	
Microsoft Encrypt	EAP types:			
🗖 Uger can c	Protected EAP (PEAP)			Move <u>U</u> p.
Encrypted auther				Move Down
Unencrypted auti				
Unauthenticated acc				
☐ Allow clients to ci method.				
	<u>A</u> dd <u>E</u>	dit <u>R</u> emove	ОК	Cancel
	OK	Cancel Apply	J	

7. Clique em Edit em Select EAP Providers e escolha, no menu suspenso, o servidor associado às suas contas de usuário e CA do Ative Diretory (por exemplo, tme.tme.com). Adicione o tipo de EAP MSCHAP v2<sup>.</sup>

Select EAP Providers			?×		N.X.C.R.S.R.S.R. D.D.X.D.X.D.N.D. 1001 G.X.D.X.D.N.D.K.D
EAP types are negotiated in the or EAP types: Protected EAP (PEAP)	Protected EAP Prope This server identifies it Select the certificate th	itties self to callers befor hat you want it to u	e the connection is completed. se as proof of identity.	2×	
	Certificate issued	tme.tme.com	1		
	Issuer:	wnbu			
	Expiration date:	3/30/2007 3:.	52:22 PM		
Add Edit	Secured password (EA	AP-MSCHAP ∨2)	EAP MSCHAPv2 Properties		×
	Add	Edit Rem	Number of authentication retries	si 2	
				Cancel	

8. Clique na guia Encryption e marque todos os tipos de criptografia para acesso

Edit Dial-in Profile		<u>? ×</u>
Dial-in Constraints Authentication	IP Encryption	Multilink     Advanced
The following encryption la Routing and Remote Acce make sure the encryption l	evels are supported by ser ess. If you use a different r levels you select are supp	vers running Microsoft emote access server, orted by that software.
If No encryption is the only using data encryption.	option selected, then use	ers cannot connect by
☑ Basic encryption (MP	PE 40-bit)	
Strong encryption (M	PPE 56 bit)	
Strongest encryption	(MPPE 128 bit)	
☑ No encryption		
	ОК Са	ancel <u>Apply</u>

remoto:

9. Clique na guia Advanced e adicione RADIUS Standard/Framed como o Service-

t Dial-in Profile		
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Specify additional connecti Access server. Attri <u>b</u> utes:	on attributes to be return	ned to the Remote
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Add	<u>R</u> emove	Þ
Add	<u>R</u> emove	
Add Edit	<u>R</u> emove	

Type:

10. Clique na guia **IP** e marque **O cliente pode solicitar um endereço IP**. Isso pressupõe que o DHCP esteja habilitado em um switch ou

Authentication   Dial-in Constraints	Encryption IP	Advance Multilink
IP address assignment (Fra	amed-IP-Address)	
Server must supply an	IP address	
Client may request an I	P address	
C Server settings determ	ine IP address assigr	nment
C Assign a static IP addr	ess 255 .	255 . 255 . 255
If an IP address assignmer overrides these settings.	nt method is specified	d in the user profile, it
IP hiters		
you can define the filters to	er is Microsoft Houtin apply during this co	ng and Remote Acces Innection.
To control the packets this click Input Filters.	s interface receives,	Input Filters
To control the packets this	s interface sends, clic	ck <u>O</u> utput Filters
Output Filters.		

WinServer."

### Configurações de segurança de domínio do Microsoft Windows 2003

Conclua estas etapas para definir as configurações de segurança de domínio do Windows 2003:

1. Inicie o gerenciador de Configurações de segurança de domínio padrão e crie uma nova política de segurança para Políticas de rede sem fio (IEEE

<u>File Action View H</u> elp	
← → 🗈 🖪 🗗 🔂 😫 🏠	
Security Settings	Name
🗄 🧬 Account Policies	WLAN Network Policy
🗄 🛃 Local Policies	
🗄 🗃 Event Log	
🗄 🧰 Restricted Groups	
🗄 🧰 System Services	
🗄 🧰 Registry	
🕀 🧰 File System	
Wireless Network (IEEE 902 11) Policies	

2. Abra as Propriedades da Diretiva de Rede WLAN e clique em **Redes Preferenciais**. Adicione uma nova WLAN preferencial e digite o nome do SSID da WLAN, como Wireless. Clique duas vezes nessa nova rede preferencial e clique na **guia IEEE 802.1x**. Escolha PEAP como o tipo de

D	
	•

WLAN Network Policy Properties	?×	
General Preferred Networks	dit sroller Properties	<u>?</u> ×
Automatically conne	Network Properties IEEE 802.1x	1
CT below.	EAPOL-Start message:	
Networks:	Parameters (seconds)	
Network Name (SSID) IEE	Max start: 3 Start period: 60 Start period: 60	
sroller E	Held period: 60. (1919) Authentication period: 30. (1919)	
	EAP type: Protected EAP (PEAP)	
	Authenticate as guest when user or computer information is unavailable	
	Authenticate as computer when computer information is available	
A <u>d</u> d <u>E</u> dit	Computer authentication: With user re-authentication	
	OK Ca	ncel

3. Clique em **PEAP Settings**, marque **Validate server certificate** e selecione o Trusted Root Cert instalado na Certificate Authority. Para fins de teste, desmarque a caixa MS CHAP v2 para Automatically use my Windows login and password (Usar automaticamente meu login e

senha do Windows)

Protected EAP Properties	?×
When connecting:	
- 🔽 Validate server certificate	
Connect to these servers:	
Trusted <u>R</u> oot Certification Authorities:	
VeriSign Trust Network	
VeriSign Trust Network	
VeriSign Trust Network	
wnbu	
wnbu	
Cert EZ by DST	
	EAP MSCHAPv2 Properties
Select Authentication Method:	When connecting:
Secured password (EAP-MSCHAP v2)	when connecting.
Enable Fast Reconnect	Automatically use my Windows logon name and password (and domain if any).
	OK Cancel

 Na janela Gerenciador de configurações de segurança de domínio padrão do Windows 2003, crie outras novas diretivas de segurança IP na diretiva do Ative Diretory, como 4404.



5. Edite as novas propriedades da política 4404 e clique na guia Rules. Adicione uma nova

regra de filtro - Lista de filtros IP (Dinâmica); Ação de filtro (Resposta padrão); Autenticação (PSK); Túnel (Nenhum). Clique duas vezes na regra de filtro recém-criada e selecione Métodos de

#### segurança:

4404 Prop	perties				?× IP traffic
Rules	General				
	a Securitor	ules for commun	icating with of	ner computers	
88	3				
IP Sec	urity rules:	-			
IP Filt	er List	Filter Actio	n	Authentication.	Tu
I < [	)ynamic>	Default R	esponse	Preshared Key	<n< td=""></n<>
Ed	lit Rule Pror	perties			?   ×
				•	
	Security Meth	nods Authentic	ation Methods	I	
	Offer these	security methods	when negotia	ating with anothe	r computer.
	Security me	thod preference	order:		
	Туре	AH Integrity	ESP Confid	dential ES	Add
Ľ	Custom	<none></none>	3DES	SH	
	Custom	<none></none>	3DES	ME	<u>Edit</u>
	Custom	<none></none>	DES	ME	Bemove
	Custom	SHA1	<none></none>	<n< td=""><td></td></n<>	
	Custom	MD5	<none></none>	<pre><n< pre=""></n<></pre>	Move up
	•			•	Move down
	Use ses	sion <u>k</u> ey perfect	forward secre	cy (PFS)	

 Clique em Edit Security Method e clique no botão de opção Custom Settings. Escolha estas configurações.Observação: essas configurações devem corresponder às configurações de segurança IPSec RADIUS do controlador.

Edit Security Method		P traffic, always req.
Security Method		
<ul> <li>Integrity and encry Data will be encry unmodified.</li> <li>Integrity only Data will be verified encrypted.</li> <li><u>C</u>ustom</li> <li><u>S</u>ettings</li> </ul>	Detion Custom Security Method Settings Specify the settings for this custom securit Data and address integrity without end Integrity algorithm: MD5 Data integrity and encryption (ESP): Integrity algorithm: SHA1	ty method. cryption ( <u>A</u> H) :
	3DES     Session key settings: <ul> <li>Generate a new key every:</li> <li>100000</li> <li>Kbytes</li> </ul>	Generate a new key every:          28800       seconds         0K       Cancel

7. Clique na guia **Authentication Method** em Edit Rule Properties. Insira o mesmo segredo compartilhado que você inseriu anteriormente na configuração RADIUS da controladora.

Rule Properties		? × P traffic, alwa
ecurity Methods Au	hentication Methods	hed
betweer offered compute	n computers. These authentication methods and accepted when negotiating security wit er.	are h another
Authentication metho	d preference order:	
Preshared Key	cisco	<u>E</u> dit
Edit	Authentication Method Properties	] []
Au	thentication Method The authentication method spe between the computers.	cifies how trust is established
(	Active Directory default (Kerberos V5 pro Use a certificate from this certification au	tocol) thority (CA): Browse.
	Exclude the CA name from the certil	ficate requesting
6	Use this string (preshared key):	

Neste ponto, todas as configurações para o Controlador, IAS e as Configurações de Segurança de Domínio são concluídas. Salve todas as configurações no Controlador e no WinServer e reinicialize todas as máquinas. No cliente WLAN usado para o teste, instale o certificado raiz e configure para WPA2/PEAP. Depois que o certificado raiz for instalado no cliente, reinicialize a máquina do cliente. Após a reinicialização de todas as máquinas, conecte o cliente à WLAN e capture esses eventos de log.

**Observação:** uma conexão de cliente é necessária para configurar a conexão IPSec entre o Controlador e o WinServer RADIUS.

# Eventos de Log do Sistema do Windows 2003

Uma conexão bem-sucedida de cliente WLAN configurada para WPA2/PEAP com IPSec RADIUS habilitado gera este evento System no WinServer:

#### 192.168.30.105 = WinServer 192.168.30.2 = WLAN Controller

😽 Event Viewer							
Eile Action View	Help						
← → 💽 💽 🖆	1 🗟 🔹						
Event Viewer (Local)	System 22 eve	nt(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Socurity	Information	4/1/2006	2:52:42 PM	IAS	None	1	N/A

```
User TME0\Administrator was granted access.
Fully-Qualified-User-Name = tme.com/Users/Administrator
NAS-IP-Address = 192.168.30.2
NAS-Identifier = Cisco_40:5f:23
Client-Friendly-Name = 4404
Client-IP-Address = 192.168.30.2
Calling-Station-Identifier = 00-40-96-A6-D4-6D
NAS-Port-Type = Wireless - IEEE 802.11
NAS-Port = 1
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = 4404
Authentication-Type = PEAP
EAP-Type = Secured password (EAP-MSCHAP v2)
```

Uma conexão IPSec RADIUS do controlador <> bem-sucedida gera este evento de segurança nos registros do WinServer:

😫 Event Viewer							
Ele Action View	Help						
⇔ ⇒ 🗈 🖬 🖀	6 🗟 😫						
Event Viewer (Local)	Security 484 ev	ent(s)					
Application	Туре	Date	Time	Source	Category	Event	User
Security System	Success Audit	4/1/2006	2:22:25 PM	Security	Logor/Logoff	541	NETWORK SERVICE

IKE security association established. Mode: Data Protection Mode (Quick Mode) Peer Identity: Preshared key ID. Peer IP Address: 192.168.30.2 Filter: Source IP Address 192.168.30.105 Source IP Address Mask 255.255.255.255 Destination IP Address 192.168.30.2 Destination IP Address Mask 255.255.255.255 Protocol 17 Source Port 1812 Destination Port 0 IKE Local Addr 192.168.30.105 IKE Peer Addr 192.168.30.2 IKE Source Port 500 IKE Destination Port 500 Peer Private Addr Parameters: ESP Algorithm Triple DES CBC HMAC Algorithm SHA

AH Algorithm None Encapsulation Transport Mode InboundSpi 3531784413 (0xd282c0dd) OutBoundSpi 4047139137 (0xf13a7141) Lifetime (sec) 28800 Lifetime (kb) 100000 QM delta time (sec) 0 Total delta time (sec) 0

# Exemplo de depuração bem-sucedida de IPSec RADIUS do controlador de LAN sem fio

Você pode usar o comando debug **debug pm ikemsg enable** no controlador para verificar essa configuração. Exemplo:

```
(Cisco Controller) >debug pm ikemsg enable
(Cisco Controller) >****** ERR: Connection timed out or error, calling callback
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x00000000000000000
SA: doi=1 situation=0x1
Proposal 0, proto=ISAKMP, # transforms=1, SPI[0]
Transform#=0 TransformId=1, # SA Attributes = 6
EncrAlgo = 3DES-CBC
HashAlgo = SHA
AuthMethod = Pre-shared Key
GroupDescr =2
LifeType = secs
LifeDuration =28800
VID: vendor id[16] = 0x8f9cc94e 01248ecd f147594c 284b213b
VID: vendor id[16] = 0x27bab5dc 01ea0760 ea4e3190 ac27c0d0
VID: vendor id[16] = 0x6105c422 e76847e4 3f968480 1292aecd
VID: vendor id[16] = 0x4485152d 18b6bbcd 0be8a846 9579ddcc
VID: vendor id[16] = 0xcd604643 35df21f8 7cfdb2fc 68b6a448
VID: vendor id[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
VID: vendor id[16] = 0x7d9419a6 5310ca6f 2c179d92 15529d56
VID: vendor id[16] = 0x12f5f28c 457168a9 702d9fe2 74cc0100
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
SA: doi=1 situation=0x1
Proposal 1, proto=ISAKMP, # transforms=1 SPI[0]
Transform payload: transf#=1 transfId=1, # SA Attributes = 6
EncrAlgo= 3DES-CBC
HashAlgo= SHA
GroupDescr=2
AuthMethod= Pre-shared Key
LifeType= secs
LifeDuration=28800
VENDOR ID: data[20] = 0x1e2b5169 05991c7d 7c96fcbf b587e461 00000004
VENDOR ID: data[16] = 0x4048b7d5 6ebce885 25e7de7f 00d6c2d3
VENDOR ID: data[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
KE: ke[128] = 0x9644af13 b4275866 478d294f d5408dc5 e243fc58...
NONCE: nonce [16] = 0xede8dc12 c11be7a7 aa0640dd 4cd24657
PRV[payloadId=130]: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6
c67
PRV[payloadId=130]: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b1
378
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
KE: ke[128] = 0x9f0420e5 b13adb04 a481e91c 8d1c4267 91c8b486...
```

```
NONCE: nonce[20] = 0x011a4520 04e31ba1 6089d2d6 347549c3 260ad104
PRV payloadId=130: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b13
78
PRV payloadId=130: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6c
67
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x04814190 5d87caal 221928de 820d9f6e ac2ef809
NOTIFY: doi=1 proto=ISAKMP type=INITIAL_CONTACT, spi[0]
NOTIFY: data[0]
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x3b26e590 66651f13 2a86f62d 1b1d1e71 064b43f6
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
SA: doi=1 situation=0x1
Proposal 1, proto=ESP, # transforms=1, SPI[4] = 0xbb243261
Transform#=1 TransformId=3, # SA Attributes = 4
AuthAlgo = HMAC-SHA
LifeType = secs
LifeDuration =28800
EncapMode = Transport
NONCE: nonce [16] = 0x48a874dd 02d91720 29463981 209959bd
ID: packet[8] = 0x01110000 c0a81e02
ID: packet[8] = 0x01110714 c0a81e69
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x2228d010 84c6014e dd04ee05 4d15239a 32a9e2ba
SA: doi=1 situation=0x1
Proposal 1, proto=ESP, # transforms=1 SPI[4] = 0x7d117296
Transform payload: transf#=1 transfId=3, # SA Attributes = 4
LifeType= secs
LifeDuration=28800
EncapMode= Transport
AuthAlgo= HMAC-SHA
NONCE: nonce[20] = 0x5c4600e4 5938cbb0 760d47f4 024a59dd 63d7ddce
ID: packet[8] = 0x01110000 c0a81e02
ID: packet[8] = 0x01110714 c0a81e69
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x0e81093e bc26ebf3 d367297c d9f7c000 28a3662d
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0xcb862635 2b30202f 83fc5d7a 2264619d b09faed2
NOTIFY: doi=1 proto=ESP type=CONNECTED, spi[4] = 0xbb243261
data[8] = 0x434f4e4e 45435431
```

#### Captura ética

Aqui está um exemplo de Captura Ética.

```
192.168.30.105 = WinServer
192.168.30.2 = WLAN Controller
192.168.30.107 = Authenticated WLAN client
No. Time Source Destination Protocol Info
1 0.000000 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
2 1.564706 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
```

```
3 1.591426 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
4 1.615600 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
5 1.617243 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
6 1.625168 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
7 1.627006 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
8 1.638414 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
9 1.639673 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
10 1.658440 192.168.30.2 192.168.30.105 ESP (SPI=0x7d117296)
11 1.662462 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
12 1.673782 192.168.30.2 192.168.30.105 ESP ESP (SPI=0x7d117296)
13 1.674631 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
14 1.687892 192.168.30.2 192.168.30.105 ESP (SPI=0x7d117296)
15 1.708082 192.168.30.105 192.168.30.2 ESP ESP (SPI=0xbb243261)
16 1.743648 192.168.30.107 Broadcast LLC U, func=XID;
  DSAP NULL LSAP Individual, SSAP NULL LSAP Command
17 2.000073 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
  Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
18 4.000266 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
  Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
19 5.062531 Cisco_42:d3:03 Cisco_42:d3:03 LOOP Reply
20 5.192104 192.168.30.101 192.168.30.255 NBNS Name query NB PRINT.CISCO.COM<00>
21 5.942171 192.168.30.101 192.168.30.255 NBNS Name query NB PRINT.CISCO.COM<00>
22 6.000242 Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf.
  Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
23 6.562944 192.168.30.2 192.168.30.105 ARP Who has 192.168.30.105? Tell 192.168.30.2
24 6.562982 192.168.30.105 192.168.30.2 ARP 192.168.30.105 is at 00:40:63:e3:19:c9
25 6.596937 192.168.30.107 Broadcast ARP 192.168.30.107 is at 00:13:ce:67:ae:d2
```

## Informações Relacionadas

- Guia de configuração do Controlador de LAN sem fio da Cisco, versão 5.2
- Suporte Técnico e Documentação Cisco Systems

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.